스마트그리드 기기를 위한 이동형 키 주입 방법에 관한 연구

현무용*, 최연주*, 이승원*
*한전KDN(주)
e-mail:my_hyun05@kdn.com, yeonju.12@kdn.com, swlee_1201@kdn.com

A study on the mobile key injection method for smart grid devices

Mu-Yong Hyun*, Yeon-Ju Choi*, Seung-Won Lee*
*KEPCO-KDN

요 약

기존 전력망과 최신 IT기술의 융합을 통해 탄생한 차세대 전력망인 스마트그리드의 확산이 본격화 됨에 따라 스마트그리드 환경 하에서 동작하는 단말기기, 운영시스템 간 보안통신에 대한 요구사항이 급증하고 있으며, 관련 연구도 활발히 진행 중에 있다. 적법한 인증과정을 거친 인가된 기기와 서버 간 안전한 통신환경 구축을 위해서는 PKI 기반의 기기 보안인증 기술의 적용이 필수적이다. 본 논문에서는 스마트 기기 간 PKI 기반의 기기 보안인증 통신을 위해 스마트 기기용 암호화 키를 안전하게 생성, 관리 및 주입하는 방법에 대해 제시한다. 제시된 방법은 스마트 기기에 대한 안전한 키 관리 및 주입은 물론, 모바일 장비를 활용한 이동식 키주입 방법을 지원함으로써 스마트 기기의 암호화키 노출 등 해킹사고 발생 시 장비교체에 따른 전력서비스 공백을 최소화 할 수 있다.

1. 서론

스마트그리드는 기존 전력망과 최신 IT기술의 융합을 통해 탄생한 차세대 전력망으로 전력 생산자와 소비자가 양방향 정보의 교류를 가능하게 하며 전력 이용효율을 극대화함은 물론 전력공급에 대한 높은 가용성과 신뢰성을 제공한다. 그러나, 기존 통신망과의 연계, 소비자단에서의 접근가능 지점 증가 등 정보통신기술의 접목에 따른 사이버 보안 취약성을 내포하고 있으며, 사이버테러 발생 시 대정전과 같은 국가 전력마비 사태가 가능하므로 관련 정보보호 기술 적용을 위한 연구가 활발히 진행 중이다[1].

또한, 스마트그리드 기기들은 넓은 공간에 산재되어 있을 뿐만 아니라 개방된 공간에 노출되어 설치되기 때문에 사이버 공격에 취약하다. 따라서 PKI 기반 기기 보안기술을 적용, 적법한 인증과정을 거친 인가된 기기 및 서버 간 안전한 통신환경 구축에 대한 연구가 필수적이다[2,3].

본 논문에서는 스마트 기기 간 PKI 기반의 기기 보안인증 통신을 위해 스마트 기기용 암호화 키를 안전하게 생성, 관리 및 주입하는 방법에 대해 제시한다. 제시된 방법은 스마트 기기에 대한 안전한 키 관리 및 주입은 물론, 모바일 장비를 활용한 이동식 키주입 방법을 지원함으로써 스마트 기기의 암호화키 노출 등 해킹사고 발생 시 장비교체에 따른 전력서비스 공백을 최소화 할 수 있다.

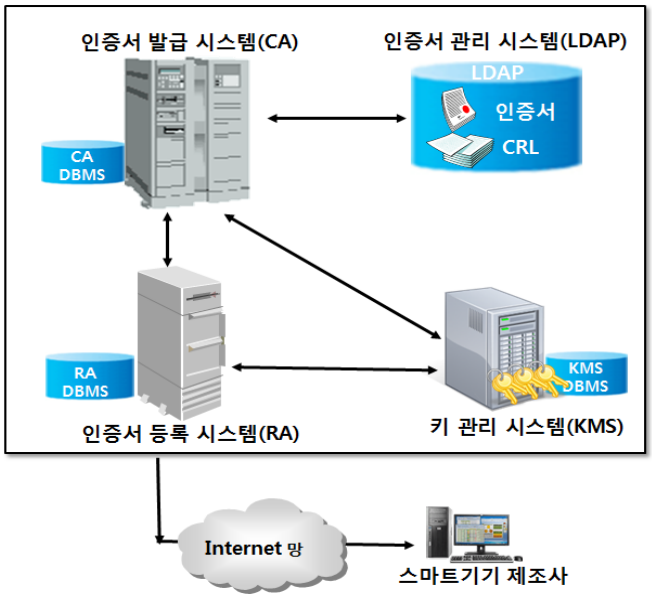
2. 본론

1) PKI 기반 기기 보안인증 운영 환경

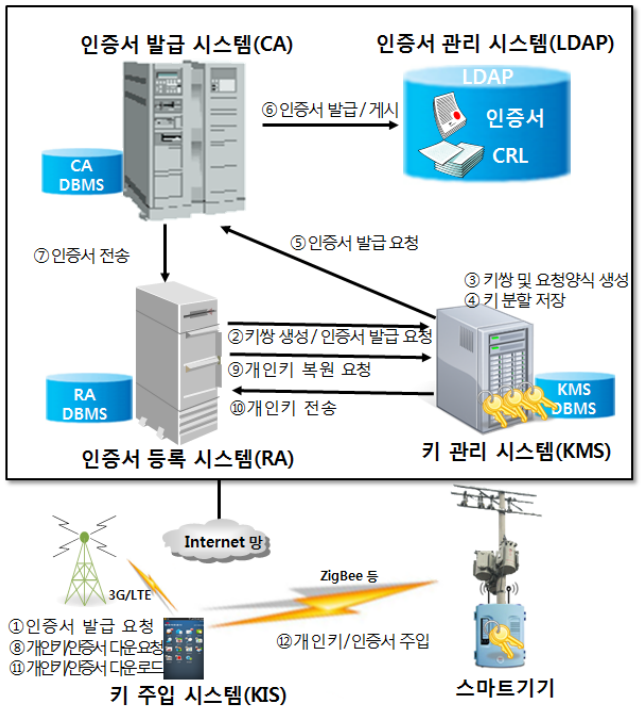
그림1은 PKI 기반 기기 보안인증 운영환경의 기본 구성을 예시하고 있다. PKI 기반 스마트그리드 기기 보안인증 운영환경은 인증서 발급시스템(CA), 인증서 관리 시스템(LDAP), 인증서 등록 시스템(RA), 키 관리 시스템(KMS)으로 구성된다. 인증서 발급 시스템은 X.509 국제표준기반으로 기기 인증서를 발급하고, 인증서 등록 시스템은 스마트기기 제조사로부터 전송된 인증서 발급요청을 키 관리 시스템으로 전달하며 발급된 인증서에 대한 다운로드 서비스를 제공한다. 키 관리시스템은 기기 인증서 발급에 필요한 키쌍(개인키, 공개키)을 생성하고 안전하게 관리하며, 인증서 관리 시스템은 발급된 인증서를 저장하고 관리하는 역할을 수행한다.

2) 인증서 발급 및 주입 절차

스마트그리드 분야 현장기기들은 보안이 취약한 노출된 환경에 설치되는 경우가 많기 때문에 사이버 해킹 가능성이 상존한다. 사이버 공격에 의해 기기 암호화키가 노출되었을 경우, 신속한 키 교체 및 인증서 갱신이 요구된다. 기존의 방식에 의하면 키 교체 및 인증서 갱신을 위해서는 대상 기기들을 철거하여 제조사로 입고시키는 과정이 수반되며, 이에 따른 막대한 비용 및 시간이 소요될 뿐만 아니라 전력서비스에 대한 공백이 불가피하다. 본 논문에서는 이러한 문제점을 해결하기 위해 모바일 기기를 이용한 인증서 발급 및 주입절차를 그림2과 같이 제안한다.



(그림 1) PKI 기반 기기 보안인증 기본 구성



(그림 2) 인증서 발급 및 주입 절차

키 주입 대상 스마트 기기는 무선통신 인터페이스(ZibBee 등)가 지원된다고 가정하며, 이동형 키주입 시스템과 스마트 기기 간에는 TLS 기반의 상호인증 및 보안 채널이 형성된다.

스마트 기기 제조사 관리자 혹은 스마트기기 유지보수 담당자는 키 주입 시스템(KIS)을 통해 스마트 기기들에 대한 기기정보를 작성한 후, 기기인증서 발급요청 메시지를 인증서 등록 시스템(RA)으로 전송한다. 인증서 등록 시스템은 제공받은 기기정보를 이용하여 키 관리 시스템(KMS)으로 기기에 대한 키쌍(공개키, 개인키) 생성 및 인증서 발급요청을 전송한다.

키 관리 시스템(KMS)은 전달받은 기기정보 및 내장 암호모듈을 호출하여 기기 개인키 및 공개키 쌍과 국제표준(PKCS#10) 기반의 인증서 발급요청 양식을 생성하고 개인키를 안전하게 분할하여 저장한다. 키 관리 시스템은 기기정보와 생성된 인증서 발급요청 양식을 포함한 인증서 발급요청 메시지를 인증서 발급서버로 전송한다. 인증서 발급요청 메시지를 수신한 인증서 발급 시스템은 인증서 발급요청 양식을 확인 후 국제표준(X.509) 기반의 기기인증서를 발급하여 인증서 관리시스템에 저장한다.

인증서 발급완료가 확인되면 키 주입 시스템은 인증서 등록 시스템으로 인증서와 개인키를 요청하며, 요청을 받은 인증서 등록 시스템은 키 관리 시스템으로 개인키 복원요청 메시지를 전송한다. 개인키 복원요청 메시지를 받은 키 관리 시스템은 키 복원요청 정보 중 기기 구분정보를 이용하여 분할 저장되어 있는 개인키를 복원한 뒤 인증서 등록 시스템을 통해 키 주입 시스템으로 전달한다.

인증서 등록 시스템으로부터 수신된 인증서 및 개인키는 키 주입 시스템(KIS)과 스마트기기 간 형성된 보안채널을 통해 안전하게 스마트 기기에 주입된다.

3. 결론

지능화된 차세대 전력망인 스마트그리드의 보급이 가속화됨에 따라, 스마트그리드 통신환경을 안전하게 운영하기 위한 보안 요구사항이 급증하고 있으며, 안전한 스마트그리드 통신환경 구축을 위한 연구들이 활발히 진행 중이다.

본 논문에서는 스마트 기기 간 PKI 기반의 기기 보안인증 통신을 위해 스마트 기기용 암호화 키를 안전하게 생성, 관리 및 주입하는 방법에 대해 제시한다. 제시된 방법은 스마트 기기에 대한 안전한 키 관리 및 주입은 물론, 모바일 장비를 활용한 이동식 키주입 방법을 지원함으로써 스마트 기기의 암호화키 노출 등 해킹사고 발생 시 장비교체에 따른 전력서비스 공백을 최소화 할 수 있다.

ACKNOWLEDGMENT

본 연구는 미래창조과학부 한국정보화진흥원의 지원을 받고 있는 “스마트그리드 보안 테스트베드 구축 및 실증” 과제에 의해 수행되었습니다.

참고문헌

[1] Salsabeel S., Fatma Q., Raafat A., “Smart grid cyber security: Challenges and solutions”, ICSGCE 2015

[2] Danda B. R., Chandra B., “Cyber security for smart grid systems: Status, challenges and perspectives”, SoutheastCon 2015

[3] Daojing He, Sammy C., Yan Z., “An enhanced public key infrastructure to secure smart grid wireless communication networks”, IEEE Network 2014